BGYS-PL-02

BİLGİ GÜVENLİĞİ ALT POLİTİKALARI

İÇİNDEKİLER

1. Amaç

Bu doküman Kapsam Analizi Dokümanında belirtilen birimlerde tüm bilgi varlıklarının güvenliğinin sağlanması, BGYS'nin kurulması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi için yönetimin yönlendirmesi ve desteğinin belirlenmesi amacı ile oluşturulmuştur.

2. Kapsam

Bu doküman, kapsamdaki tüm bilgi varlıklarını ve bilgi varlıklarının güvenliğini kapsamaktadır.

3. Revizyon Kayıtları ve Doküman Onayları

Revizyon No	Tarih	Revizyon Nedeni	Revizyon Sayfa No	Revize Edilen Bölüm

3.1. Doküman Onayları

Hazırlayan	Kontrol Eden	Onaylayan
YUSUF EĞRİ Bilgisayar Programcısı	AYHAN ÖZDEMİR Bilgi İşlem Daire Başkanı	Prof.Dr. ALİM YILDIZ Rektör

4. Tanımlamalar ve Kısaltmalar

Kısaltmalar ve tanımlamalar kılavuzunda belirtilmiştir.

5. Uygulama

Bu politika dokümanı Kurumumuzun uygulayacağı bilgi güvenliği kontrollerine ait genel yaklaşımını yansıtmaktadır ve uygulanacak kontrollerin hayata geçirilmesini sağlayacak prosedürlere yön verecektir. Bu politika prosedürler ile desteklenerek kurumumuzda etkin ve sürekli iyileştirme sağlayan bir Bilgi Güvenliği Yönetim Sistemi sürdürülmesini sağlayacaktır.

5.1. Erişim Kontrol Politikası

Bilgi güvenliğini sağlamanın en temel yolu, bilgi varlığına yetkisiz kişilerin erişimlerini engellemek ve yetkisi olan kişilerin erişimlerini de ihtiyaca göre kısıtlamaktır. Bu erişimler, fiziksel ve mantıksal erişim olarak iki şekilde denetlenir. Erişim kontrollerinde yasal gereksinimler göz önünde bulundurulur ve varlık sınıflandırmasına uygun yetkilendirmeler yapılır. Gerektiği kadar bilme prensibi ve açıkça izin verilmedikçe her şey yasaktır kuralı Kurum erişim yönetiminin temelini oluşturur.

5.2. Varlıkların Kabul Edilebilir Kullanımı

Kurum iş süreçlerinin yürütülmesinde yalnızca Kurum bilişim kaynakları kullanılır. Bu kaynakların kullanımında esas Kurumun araştırma, geliştirme, toplumsal hizmet ve idari/yönetimsel faaliyetleri ile doğrudan ilişkili olan kullanımdır. Kurum kaynaklarının kullanımı, mevzuata ve Kurum politika ve prosedürlerine aykırı olamaz. Varlıkların kullanımında yasal gereksinimler, gizlilik, bütünlük ve erişilebililik kavramları göz önünde bulundurularak güvenlik riskleri incelenir ve önlemler alınır.

5.3. Mobil Cihaz Politikası

Mobil cihazların güvenlik zayıflıkları diğer bilişim sistemlerine ek zafiyetler içerdiğinden iş süreçlerinin mecburi gereksinimleri göz önünde bulundurularak kullanılır. Mobil cihaz kullanımı sırasında risk analizleri gerçekleştirilerek kullanım kısıtlamaları ve ek teknolojik önlemler ile güvenlik gereksinimleri sağlanır.

5.4. Kriptografik Kontroller Politikası

Kriptografik kontrollerin uygulanmasında yasal gereksinimler öncelikli incelenir ve risk analizleri ele alınır. Teknolojik olarak desteklenen tüm sistemlerde işlediği veri sınıfına uygun şifreleme yöntemleri kullanılır. Şifreleme yöntemlerinin seçiminde güvenlik gereksinimlerini sağlayacak güncel algoritmalar ve uygun anahtar yönetim süreçleri işletilir.

5.5. Bilgi Transfer Politikaları

Bilgi transferinde bilgi sınıflarına uygun olarak kriptografik kontroller, fiziksel ve mantıksal erişim kontrolleri uygulanır. Bilgi sınıflandırmasında mutabakat yapılması, transfer edilecek bilginin tanımlanması, paylaşım sonrası kullanım süresi ve fikri mülkiyet hakları konuları dokümante edilir ve kayıt altına alınır.

5.6. İnsan Kaynakları Disiplin Kuralları

Tüm personele mevzuat gereği ve Kurum Bilgi Güvenliği politika, prosedür, talimat, taahhütname vb. şartlarına uymadığında ilgili disiplin süreci başlatılır.

5.7. Parola Politikası

Kurumda kullanılan tüm parolalar uluslararası standartlara uygun güvenlik seviyeleri göz önünde bulundurularak belirlenir ve kullanılır. Belirlenen bu seviye tüm parola gerektiren sistemlerde uygulanır. Parolanın kişiye özel olduğu paylaşılmaması ve tahmin edilemez olması kullanıcıların sorumluluğundadır.

5.8. Temiz Masa Temiz Ekran Politikası

Gizli ve üzeri bilgi sınıfındaki evraklar, parolalar, taşınabilir depolama ortamları, bilgi ve belgeler masa üzerinde, yazıcı, faks gibi cihazlarda ya da kolayca ulaşılabilir yerlerde bırakılmaz. Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenerek çalışma ortamlarında veri güvenliği şartlarını kontrol etmek personel sorumluluğundadır.

5.9. Güvenli Geliştirme Politikası

Kurumda kullanılacak uygulamaların ve sistemlerin seçiminde ve geliştirmesinde dünya çapında kabul görmüş standartların uygulanması ya da bu standartlara uygun olan uygulama ve sistemlerin temini sağlanır. Bu bağlamda; Geliştirme yaşam döngüsü içerisindeki sistem değişikliklerinin kontrolü, işletim platformu değişikliklerinin kontrolü, yazılım paketlerindeki değişikliklerin kontrolü, güvenli sitem mühendisliği prensipleri, Güvenli geliştirme ortamı, sistem güvenlik testleri, sistem kabul testleri, test verisinin güvenliği kontrolleri uygulanır.

5.10. Tedarikçi İlişkileri Bilgi Güvenliği Politikası

Kurum, iş süreçlerinin işleyişini, devamlılığını ve kalitesini arttırmak için tedarikçiler ile çalışmalar yapmaktadır. Yapılan bu çalışmalar esnasında çalışma şartlarının belirlenmesi ve dokümante edilmesi hem Kurumun hem de tedarikçinin sorumluluğundadır.

Tedarikçi ilişkilerini yönetmek için, alınan mal ya da hizmetler bilgi güvenliğini etkileyecek türde ise, her birim kendi risk eğilimine ve çalışacağı tedarikçinin türüne göre tedarik sürecini planlar. Süreç dâhilinde bilgi varlıklarına erişim türünü belirler, verilen erişim izinlerini izler, Kurum politika ve prosedürlerine uyumu sağlar ve bilgi güvenliği farkındalığını arttırmak için gerekli uygulamaları gerçekleştirir.

Tedarikçi anlaşmaları ile Kurum ve tedarikçi arasında yanlış anlama olasılığının ortadan kaldırılmasını sağlamak ve bilgi güvenliği gereksinimlerini yerine getirmek için her iki tarafın da yükümlülüklerine ilişkin dokümante edilmiş belge oluşturulur ve saklanır.

6. İlgili Dokümanlar

6.1. İç Kaynaklı Dokümanlar

1. Kapsam Analizi Dokümanı

6.2. Dış Kaynaklı Dokümanlar

1. TR EN ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı